1.0 PURPOSE

This policy prescribes the measures required to counter computer viruses and identifies the responsibilities in protecting the State network against malicious software. This protection includes the tools and procedures necessary to prevent major and widespread damage to user applications, files, desktops, workstations, and laptops/notebooks, which are either physically or remotely connected to the State network via a standard network, wireless, modem, or through virtual private network (VPN).

2.0 SCOPE

This policy applies to all employees within the Executive Branch, unless classified as "exempt" in West Virginia Code Section 5A-6-8, "Exemptions." The State's users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services. This policy also covers all workstations, portable computers, servers and other computing devices that attach to the State's networks.

3.0 POLICY

3.1 Malicious code protection mechanisms will be employed at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network where feasible.

3.1.1 Any information system that stores, processes, or transmits Federal Tax Information (FTI), Personal Health Information (PHI), or Personal Identity Information (PII) must be protected against malicious code transported by electronic mail, electronic mail attachments, Internet accesses, or other common means.

3.1.2 Data and program files that have been electronically transmitted to a WVOT-supported computer from another location, whether internal or external, will be automatically scanned for viruses/malware.

3.2 WVOT will evaluate, procure, install, and maintain anti-virus software and/or tools for use on all WVOT supported equipment.

3.2.1 All software **must** be installed by WVOT authorized employees.

3.2.2 Employees will only use software provided by the State.

3.3 Employees must not intentionally introduce a virus onto State computing equipment or systems, or withhold information necessary for effective virus control procedures.

3.4 Employees must not attempt to alter or disable anti-virus software, or attempt to terminate any scan being performed by anti-virus software, on any system attached to the Executive network.

3.5 Employees should use extreme caution when executing programs or opening e-mail attachments that:

3.5.1 Have not been requested; or

3.5.2 Come from an unknown source.

3.6 Employees will immediately notify the WVOT Service Desk if they have reason to believe their device may be infected with a virus or malware.

3.7 Incidents involving malicious code shall be resolved in accordance with WVOT Procedure Anti-Virus Response PO1014.

3.8 The WVOT will configure systems to prevent users from disabling anti-virus software updates and virus scans.

3.9 Scans of computers and systems will be performed weekly, at a minimum.

3.10 Real-time scans must be performed on files from external sources that are downloaded, opened, or executed in accordance with agency security policy.

3.11 Known malicious code and software will be blocked or quarantined.

3.12 WVOT will manage malicious code protection mechanisms and automatically update these protection mechanisms as needed.

4.0 RELEVANT DOCUMENTS/MATERIALS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03

- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 POLICY-SPECIFIC DEFINITIONS

6.1 Anti-Virus Coordinator – The person designated by the CTO to monitor and coordinate anti-virus activities within Executive Branch agencies.

6.2 Anti-Virus Software – Software that defends a PC against viruses and other malicious Internet code by scanning incoming attachments in e-mail and from other programs.

6.3 Anti-Virus Team Lead – The functional supervisor of the Anti-Virus Team.

6.4 Computer Virus – A piece of potentially malicious software that is designed to cause some unexpected or undesirable event, and is generally introduced to a system without the knowledge or consent of the user.

6.5 Scan – To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors, et. al.).

6.6 Workstation – A personal computer; also called a PC.

7.0 CHANGE LOG HISTORY

- July 1, 2015 --
  - Changed Policy name from “Anti-Virus” to “Malicious Software Protection”; Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions; Added Sections 4.9 through 4.12; 4.9) Scans of computers and systems will be performed weekly, at a minimum. 4.10) Real-time scans must be performed on files from external sources that are downloaded, opened, or executed in accordance with agency security policy. 4.11) Malicious code and software will be blocked or quarantined. 4.12) WVOT will manage malicious code protection mechanisms and automatically update these protection mechanisms as needed.